

S. L. Nelson, "Sex Work and Social Media: Policy, Identity, and Privacy in Networked Publics and Counterpublics," *Lateral* 8.1 (2019).

<https://doi.org/10.25158/L8.1.4>

This content is licensed under a Creative Commons Attribution 4.0 International License. Copyright is retained by authors.

Issue 8.1 (Spring 2019)

Sex Work and Social Media: Policy, Identity, and Privacy in Networked Publics and Counterpublics

S. L. Nelson

ABSTRACT Using the online practices of sex workers as a focal point, this project examines how the public/private dichotomy is governed and complicated within Social Networking Sites (SNS). It concentrates in particular on Facebook and FetLife, arguing that the former functions as a normative public and the latter as a counterpublic due, in part, to the differing regulations each site implements regarding sex work. The project centers on a qualitative study of the rhetorical strategies online sex workers use to self-identify and self-advocate, as well as the tactics they employ to maintain privacy and avoid the phenomenon of "context collapse." Through the results of this study, I discuss the theoretical and practical implications of end user cyber security tactics, considering the scholarship on digital surveillance and privacy. In addressing these strategies, it underscores the importance of privacy specifically for vulnerable populations of digital publics.

For many Social Networking Site (SNS) users, privacy is desired, but for sex workers, it is a necessity. As a result, sex workers often engage in end user cyber security tactics that illustrate possibilities and challenges for a general population of SNS users. Using the online practices of sex workers as a focal point, this article examines how privacy is governed and complicated within SNS publics. I present a qualitative study of the rhetorical and technological strategies that site users who are involved with or adjacent to sex work communities use to self-identify, as well as the cyber security tactics they employ to maintain privacy and avoid the phenomenon of "context collapse."¹ I begin by describing the sites used for the study, Facebook and FetLife, and by discussing the affordances and limitations of networked publics and counterpublics, considering each site's approach to data collection. I then provide a review of the domestic legislation regarding sex work insofar as it relates to offline and online spaces, as well as an analysis of each website's policy regarding sex work. Through the results of this study, I discuss the theoretical and practical implications of end user cyber security tactics, considering the scholarship on digital surveillance and privacy.

This article makes a dichotomous intervention. First, I expand the conversation surrounding digitally networked publics to distinguish between normative publics and counterpublics. Second, I locate and examine the intersection between online sex work, surveillance, and privacy as it exists within these publics. A great deal of scholarly work has considered the ways in which sex workers manufacture and manage their professional identities; I extend this scholarship to provide a more detailed account of the methods online sex workers use to maintain these identities within and between digitally networked publics. In addressing these strategies, I underscore the importance of privacy specifically for vulnerable populations of digital publics.

Site Description: Facebook and FetLife

Individuals involved in online sex work typically maintain multiple profiles across social networking platforms, apart from those specifically dedicated to sex work, for both personal and professional reasons.² In this section, I provide an in-depth analysis of the sites Facebook and FetLife in terms of their approaches to data collection and the ways in which they regulate and limit expression regarding sex work. These sites represent disparate policies and popularity amongst users, and surveys distributed to users through each platform provided a productive variation in results.

Bridging multiple social circles, Facebook is an SNS that encourages its users to connect with family members, friends, and acquaintances from different stages and circles in the user's life.³ During registration, Facebook requires users to sign up with "the name they go by in everyday life," and, in tension with that requirement, then clarifies that it should be a name that also appears on the user's official ID (e.g. a driver's license, passport, etc.).⁴ In 2011, Facebook introduced its "Timeline" feature, and switched from what José van Dijck identifies as a database model to that of a narrative model by encouraging users to fill in personal details to construct their own unique stories.⁵ Christian Fuchs further observes that, employing web 2.0 surveillance tactics, the site then uses this data to "[tailor] advertisements to the consumption interests of the users."⁶ Demanding information and authenticity from its users, Facebook operates by transforming public identities into marketable data.

Proclaiming itself to be "like Facebook, but run by kinksters like you and me," FetLife is an SNS centered on the expression of user sexuality. FetLife is openly geared towards participants in the BDSM lifestyle, but sets itself apart from dating sites by encouraging platonic and community-driven connections, as well as romantic and sexual ones.⁷ FetLife does not require users to provide their "real names." In fact, it claims, "some people don't mind you using their full real name and others don't want you to even use their first name," and encourages users to respect others' levels of comfort.⁸ Unlike Facebook, FetLife did not fully switch over to the "narrative model" indicated by Van Dijck, and it still functions very much as a database. Though the site presents the user with advertisements, these are typically randomized materials from the site's sponsors rather than content catered to the user through a series of algorithms. Though similar in structure, these sites operate as inherently different publics due to their disparate approaches to surveillance and data collection and to the adaptation of federal prostitution legislation into site policy.

Networked Publics and Counterpublics

The theoretical framework of networked publics and counterpublics serves as a helpful tool for understanding the meaningful differences between these two sites. Michael Warner explains that a public is formed "by the virtue of being addressed" by an external factor, such as a speaker, a performance, or even a text, and the web of discourse it incites.⁹ In the case of SNS, sites and the networks they constitute hail users in subjectivity. danah boyd further defines networked publics as "publics that are restructured by networked technology," and states that they allow users to create a public or semi-public profile, articulate a list of connections, and interact with other members of the system.¹⁰ While meeting the same qualifications as a traditional public, digitally networked publics operate as a specific subset of the category that adhere to their own structural rules.

Just as in non-digital publics, subjects of digitally networked publics employ various rhetorical tactics to appropriately navigate, express themselves, and interact with other members of the public. Speaking to a phenomenon they call "context collapse," which occurs when an audience of real, potential, and imagined viewers from various social circles of the user's life overlap, Marwick and boyd note that users in networked publics

rely on tactics such as “impression management,” “self monitoring,” and shifts in self-presentation in order to construct their identity in a way to cater to the expectations of each all at once.¹¹ Van Dijck observes, however, that because these sites are typically structured in a way that calls for an authentic identity across all platforms, maintaining separate identities on each is a challenge.¹²

While both Facebook and FetLife function as networked publics in which users rely on these methods to avoid context collapse, the types of publics hailed dictate the extent to which users must employ such methods. Warner explains that, while counterpublics meet the same criteria as publics, they are also conceptually dissimilar by merit of the facts that are “formed by their conflict with the norms and contexts of their cultural environment.”¹³ He further states that they “differ markedly in one way or another from the premises that allow the dominant culture to understand itself as a public.”¹⁴ Because counterpublics are actively in conflict with normative publics and strive to set themselves apart from the limits of such, the privacy of their members is imperative, thus complicating Van Dijck’s conjecture that digitally networked publics will consistently attempt to cohere their users’ identities between platforms.

Facebook and FetLife operate as disparate publics. Jansson et al. note, “No longer do we have one major national public sphere (cf. Habermas 1989); rather, with the emergence of social media the mediatized public sphere has become splintered into numerous smaller public spheres.”¹⁵ Not only does Facebook function as a normative public sphere and FetLife as a counterpublic sphere due to each site’s purpose (i.e. Facebook as a place to connect with friends and family and FetLife as a space to meet other members of the kink community), but they also differ in relation to their conduct regarding data collection and surveillance. In defining surveillance capitalism, Zuboff explains that it monetizes data obtained through surveillance.¹⁶ Facebook adheres to this model because, as Fuchs observes, “it stores, compares, assesses and sells the personal data and usage behaviour of several 100 million users.”¹⁷ As a result, the power dynamic between the site and its members is unidirectional; by creating an account with Facebook, the user agrees to part with their data for the company’s profit.

If this system is the norm, then FetLife, as a counterpublic, acts in conflict to it. It does so first through its refusal to collect accurate data about its members, thus providing them with an extra layer of protection against context collapse. Second, it does so through its privacy policy, which claims to only share personal information with “certain trusted third parties to perform functions and provide services to [the site] . . . but only to the extent necessary to perform these functions and provide such services.”¹⁸ The policy goes on to state (from the perspective of the site managers), “Our personal information is on FetLife as well, we would never use companies that don’t share a similar privacy philosophy as us.”¹⁹ While FetLife does not elaborate on these third parties, it makes a rhetorical effort to establish itself as separate from surveillance-based publics both through its claim to data collection as intrinsic to functionality and through its managers’ self-identification with the site’s members. The distinction between Facebook and FetLife as publics is further defined in each site’s implementation of domestic sex work legislation within their policies.

Domestic Sex Work Legislation and Site Policy

Enforcing legislation within online arenas is a tricky situation at best, and legislation pertaining to sex work is no exception. Here, I will broadly outline United States prostitution regulation before delving into the nuances of this type of labor and discussing how each SNS addresses it. Within the US legal system, sex work is regulated on a state-by-state basis. With the exception of eleven counties in Nevada in which it is legalized (a

labor status that comes with its own set of rules and limitations), it is criminalized to varying degrees across the nation.²⁰ Legally, sex work is framed as “prostitution” as a means of differentiating it from human trafficking, which extends beyond the sex trade and encompasses all forms of enforced labor, including that performed by “domestic, agriculture, and sweatshop workers.”²¹ The United States Department of Justice further defines prostitution as “a sexual act or contact with another person in return for giving or receiving a fee or a thing of value,” but these laws also tend to also encompass pimping, pandering, and commercial sex, or sexual acts either consensually or coercively exchanged for capital.²² Though this definition is applicable to most types of sex work, it is disproportionately enforced in the street-based sector.²³

The conflation of sex work human trafficking in the legislative sphere has detrimental effects on the community, especially in the online sector. In April 2018, U.S. politicians signed both the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) and the Stop Enabling Sex Traffickers Act (SESTA) into law.²⁴ Despite the well-intentioned rhetoric of the legislation’s nomenclature to prevent human trafficking, it is clear that FOSTA and SESTA are less concerned with the righteous defense of the archetypical female victim and more focused on limiting both the protections, operations, and rights of those who intentionally and willingly engage in sex work, and more broadly, the freedom and neutrality of the Internet. First, there are already substantial legislative provisions that oppose human trafficking in the United States, namely the Victims of Trafficking and Violence Protection Act, and these new bills do little to further their scope of this protection. Additionally, before the bills were even signed, mainstream news sources were quick to report that federal authorities succeeded in seizing and taking down Backpage—a site that many sex workers used for advertising.²⁵ By reducing the more popular sites through which sex workers connect with their clients, this legislation reduces the chances of authorities locating victims of human trafficking due to the erasure of sexually explicit ads while simultaneously forcing professional sex workers to either promote their services on more illicit sites or return to street-based options. In part due to this continued legislative focus on online spaces, SNS platforms adjust their policies to adhere to the law.

Facebook is clear and direct in its restrictions pertaining to online sex work. Many of its restrictions relate directly to United States law; however, some take an extra step to prohibit online sex work that is not strictly illegal (e.g. prohibiting advertising for users not in the United States, banning content that does not fall under US prostitution law, etc.). Echoing the concerns of sex work abolitionists and human trafficking legislation, it explicitly prohibits users from posting sexual content involving minors. It also removes content involving sexual violence and pornography, which is arguably in line with United States Code 18, section 1460–2252C. However, it also goes as far as prohibiting the sharing of content containing nudity and “descriptions of sexual acts that go into vivid detail,” content which typically is not strictly prohibited on sites that do not cater to minors. Most relevantly, Facebook bans both prostitution and the solicitation of escort services.²⁶ In doing so, it constructs a blanket of censorship over all forms of online sex work.

Like Facebook, FetLife complies with United States law regarding prostitution (despite being owned by the Canadian company, BitLove), but it allows users to engage in other forms of online sex work. Its Terms of Use explicitly state that the site does not allow users to “solicit or sell any kind of sex for hire.” However, in strict contrast to Facebook’s policy, it does allow users to post explicit sexual content (e.g. amateur pornographic photos and videos, erotic writing, etc.) as long as the participants are eighteen or older. Moreover, it says nothing about escort services and even permits users to create groups

to explicitly “post the schedule, price list or phone number of a phone sex operator, professional Dominant or professional submissive,” though it does not allow such information to be “publicly” posted beyond these groups.²⁷ In doing so, FetLife constructs itself as a more welcoming space for those involved in online sex work.

Online Sex Work

Beginning in the 1990s, the majority of sex work began to transition rapidly from the streets to the Internet.²⁸ Drucker and Nieri report a 50% growth in the online sector of the sex work industry between the years 1998 and 2008, and it has only expanded since then.²⁹ As a result, the scholarship on sex work has adapted to address the unique issues that arise with this shift. Earlier work on the subject has the tendency to treat sex work as inherently and inescapably violent, patriarchal, and coercive.³⁰ However, Comte notes that coercive and trafficking practices “constitute only a small portion of the reality of sex work,” and Weitzer claims that such a perspective “denies workers’ agency.”³¹ Similarly, Walby acknowledges that the rise of online sex work requires workers to perform more affective labor (e.g. the “girlfriend experience”), but also provides them with greater affective and emotional rewards.³² Centering the agency of the sex worker, I provide a review of the literature in this section that encompasses the distinctions between the different forms of online sex work, the subject positions of those in the industry other than that of the female worker, the safety and social benefits of using the Internet to conduct or mediate this form of labor, and the strategies that these workers use to avoid the risks common to this environment.

The online sex work industry has many different facets. It is typically categorized as a form of indoor sex work (as opposed to the more traditional street-based work), but this broader category also includes brothel workers, call girls, and bar hustlers.³³ Jones further distinguishes between two types of online sex work. The first involves “the use of the Internet to actually deliver a service.”³⁴ This labor includes webcam modeling, phone sex, and virtual reality experiences.³⁵ The second type refers to “the use of the Internet to market sexual services that are delivered in physical space.”³⁶ Most commonly, workers in this category use the Internet to facilitate eventual in-person interactions (e.g. by marketing services, screening clients, making appointments, etc.).³⁷ Although workers in the first category face fewer legal risks than those in the second as the services they provide are not typically illegal, privacy is crucial for both groups as they move between digital publics both for the protection of their other identities and jobs and also for their safety.

With the rise of online sex work, researchers have also broadened the scope of the field’s focus to account for the experiences of others in the industry apart from female sex workers, on whom most of the literature was originally concentrated. For instance, Holt and Blevins consider the digital discourse and communities available to clients of sex workers.³⁸ Additionally, in the realm of male sex work, Pruitt provides a review of escort ads, Blackwell and Dziegielewski discuss the health risks specific to these individuals in the industry, and McLean considers the networks available to male sex workers in Australia.³⁹ Moreover, claiming that the “literature on online sex work . . . has been restricted by society’s binary logic of gender,” Jones advocates for further research regarding the situation particular to transgender workers.⁴⁰ Keeping this suggestion in mind, I developed my survey with an open-ended question about participant gender in order to consider representatives from across the spectrum.

Sex workers report many benefits to conducting their business online. These include finding greater enjoyment in the work, the ability to reach a wider audience at a lower cost, and the ability to screen clients before engaging in business with them through

search engines and both digitally mediated and word-of-mouth exchanges with other sex workers.⁴¹ Furthermore, although online sex work contains its own range of high-risk scenarios, from outcalls with strangers to unsafe sex practices, the threat of violence and arrest is considerably lower in this segment of the industry.⁴² The Internet also offers opportunities for online sex workers to network with one another and share their experiences. McLean's study suggests that while many male sex workers are resistant to forming these networks, there are "potential benefits of associating with others on the basis of shared experience."⁴³ In her research on webcam models, Jones examines how these workers use online discussion boards to provide new models with information about the risks and rewards of the job and advice to models who encounter work-related dangers, such as doxxing, capping, and harassment.⁴⁴ Addressing the politics of the work, Feldman's analysis of the blog *Bound, Not Gagged* depicts how these sex worker community networks can develop into activist groups intent on distributing information and enacting policy change. Online spaces, however, come with risks as well as benefits.

Online sex workers face external and internal threats in the profession. Law enforcement agencies have myriad techniques for locating individual online sex workers. For instance, "classy website[s] with alluring photos and skillfully written ads," phishing software, or large sums of money deposited in PayPal accounts might draw police attention.⁴⁵ Bass's interviewees report a number of tactics they use to detect undercover police and avoid arrest, including deploying a waiting period before meeting with new clients, requiring clients to cross state lines, and even offering free sessions to known police officers.⁴⁶ Next, although, as Sanders indicates, sex workers use identity management techniques to separate their work from their personal lives (e.g. exclusion of certain sex acts, use of condoms, performing a specific sexual role, and preventing emotional intimacy with clients), McLean states that these is still an observable "negative impact of engagement in commercial sex upon the private sex lives" of these workers.⁴⁷ Finally, Jones notes that online sex workers are still at risk of verbal and physical harassment from clients and asks, "Will individual workers' ability to use technology affect their ability to protect themselves?"⁴⁸ My study addresses this question by locating and examining the specific rhetorical and technological strategies that online sex workers use to protect themselves in these diverse digital publics.

Method

A queer methodology is valuable for this type of work due to its theoretical and ethical investments. Brim and Ghaziani write, "queer social research methods question the origins and effects of concepts and categories rather than reify them in an allegedly generalizable variable-oriented paradigm, because these categories do not always align with lived experiences."⁴⁹ In this study, I question and challenge the normative, neoliberal narratives perpetuated by the surveillance-oriented agendas of web 2.0 social networking sites. My participants' lived experiences offer productive outlets for intervening in this ideology. Queer methodologies also forefront an ethical researcher-participant dynamic. Drawing on the methods presented by both queer theory and rhetoric scholars, Dadas outlines an ethical approach to entering various online public and semi-public spaces, maintaining transparency in terms of both one's identity as a researcher and the details of the study, and distributing surveys in a way that ensures the subjects' knowledge and willingness to participate.⁵⁰ Jones takes this claim a step further in her chapter on queer methodology and sex work, advocating for autoethnography in queer methodology especially as it pertains to sex work research.⁵¹ Throughout conducting this research, I maintained transparency regarding my subject position as a researcher and a member of these digital publics.

Beyond a queer methodology, I also draw on previous research regarding online sex work to present and discuss my results. Jenkins claims, "Internet technology can offer an opportunity to extend the scope of sex work research into new territories by providing a platform for the voices of people working in areas of the industry about which little is known."⁵² Through the technological slant of this study, I examine the "new territory" of online privacy practices used by sex workers in digital publics. Following McLean's lead, I use a qualitative approach to data collection and analysis "as it [is] considered to be effective in identifying nuanced and detailed information concerning the highly personal experiences of this group."⁵³ I ensured that my survey questions were open-ended in order to be receptive to this nuance. This is especially relevant to my demographic question about participant gender as, drawing on Jones's observation regarding the underrepresentation of transgender workers' experiences in the literature, I find it important to reintegrate these voices.

In order to recruit participants for this study, I began by emailing the moderators of four popular Facebook groups. I introduced myself, stated my intentions as a researcher, and asked permission to distribute my survey on their sites. Of these, the Sex Workers Outreach Project USA (SWOP-USA) group responded and maintained contact. After receiving Institutional Review Board approval for the project, I worked further with my contact from SWOP-USA to ensure that my approach to working with this community was ethical, clear, and respectful. Following Dadas's emphasis on ensuring the subject's knowledge and willingness to participate, I both requested consent through the participation script on the landing page of the survey and included an additional question that gave the participant the option to either grant me consent to quote their survey responses verbatim or only allow me to use their data in aggregate. After approving my survey questions, my SWOP-USA contact distributed the survey through their SNS networks.

I contacted the FetLife administrative staff with the same request. After receiving Institutional Review Board approval, composing a formal project proposal, and developing a profile on the site, I received permission to distribute a link to the offsite survey on my profile and through specific boards. Due to the sensitive nature of the site, anonymity is valued highly in the FetLife community. In order to gain the trust of the site users and maintain the level of transparency for which Dadas advocates as well as the autoethnographic intervention suggested by Jones, I posted my legal name, my role as a researcher, and my involvement in the FetLife community on my profile, as well as the approved post and link to the survey. I then contacted the moderators of six boards, and received permission to post from the moderator of a popular group page. I introduced myself in the group (using both my legal name and username), provided information about the study, and distributed the link on this board.

The sample included adult individuals who identify as within or adjacent to professional BDSM and/or sex work communities. The survey was open for six months between October 2017 and April 2018, and twenty-five participants responded. Participants were recruited from the groups and pages on the aforementioned sites. Partial responses were recorded, since not all participants responded to every question. I did not record any identifying information (e.g. legal name, pseudonym, IP address) from survey participants, so the locations of many of the participants are unclear (i.e. they could be situated beyond the United States). Participants were not compensated for their participation.

I gathered data on the following categories. With regard to demographic information, I asked for participant age, identity as a sex worker, and gender identity. In terms of involvement in digital publics and privacy tactics, I asked which networking sites these participants typically use for personal and professional reasons, whether or not they take

additional precautions in maintaining their privacy and anonymity across social networking platforms, and the language they use to discuss their experiences online. Due to the relatively small sample size, it is impossible to make generalizations about online sex workers as population from the results of this study. However, my study offers new qualitative data about the privacy practices these participants employ upon which further research can be founded.

The survey reflected a wide variety of demographics in terms of participant response. Participant ages ranged from 20 to 71 with a mean of 36. In terms of gender identity, eleven participants identified as female, eight identified as male, four identified as transgender or genderqueer, one identified as intersex (IS), and two did not respond. I asked whether or not the participant identified as a sex worker. Seventeen responded, "Yes," five responded, "Sometimes/It's Complicated," one responded, "No," and two did not respond. The following sections record my findings within the categories of site usage, identity management and context collapse, and surveillance, privacy, and cyber security.

Site Usage

The participants were asked two questions about the SNS platforms they used for personal reasons and those they use for discussing sex work. Due to the sites chosen for the survey, it is unsurprising that Facebook and FetLife were the sites most frequently indicated for these uses. Fifteen participants reported that they used Facebook for personal reasons specifically, and nine participants responded that they used FetLife. Some justified their use of social media. One participant stated that she uses "Facebook for interacting with friends/family." Another explained that she uses Facebook, Twitter, Instagram, and Tumblr to maintain connections with friends and her community, but does not post content. She also noted, "I also have a FetLife account, I'm a lifestyler." These initial responses underscore the claim that different communities form within different digital publics; Facebook operates as a space for individuals to connect with friends, family, and those in their local community, and FetLife as a place for those interested in maintaining a kink lifestyle.

The distinction between the two sites is further apparent in the participants' responses to the question regarding which sites they use to discuss sex work, journal their experiences, and/or support sex workers in a community setting. Eleven participants indicated that they used FetLife, and four stated that they used Facebook. Two participants provided caveats regarding the use of Facebook in this context. One clarified that he uses "secret facebook groups." Another observed, "Facebook, which pains me – it's a very insecure platform," but further remarked that, because of the site's large user base, she finds it to be a useful avenue for weighing in on the "bad information circulating in sex work communities about how to protect yourself with jerk clients and exploitative streaming platforms." The anxiety surrounding Facebook's lack of security due to its surveillance-based model is palpable in these responses. However, the site also acts as a useful platform for sex workers who are involved in the political side of the profession, such as those on which Feldman's study focuses, to share their views. Jansson et al. observe, "networked communications . . . facilitate an easy and affordable dissemination of information of the kind unlikely to circulate in traditional media."⁵⁴ Because Facebook is a massive SNS that encompasses a diverse range of groups, it allows those interested in spreading information greater opportunities for outreach than a smaller, more homogenous site like FetLife.

Fuchs notes that, with the rise of mass surveillance within a web 2.0 framework, the importance of community building/maintenance and collaborative information production in digital spaces has grown.⁵⁵ Although multiple groups can exist within one

digital public, not all digital publics have the infrastructure required to meet the privacy needs of each of their members. Bennett astutely states, “Individuals are arguably placed at risk because of their membership in, or assignment to, certain groups, rather than on the basis of their individual identities and the personal information it generates.”⁵⁶ Thus, it is crucial for sex workers, as a vulnerable population who face particular risks on the basis of their membership within this group, to foster communities within digital publics that can provide them with security. For these participants, Facebook exists as a public for them to correspond with “friends/family” outside of their profession, and FetLife—a counterpublic—as a space where they could safely describe their work. These findings are further reflected in the responses regarding identity management and the avoidance of context collapse.

Identity Management and Context Collapse

Identity management is a crucial tactic for sex workers, but it is one that becomes complicated as they operate in digital publics. Building off Hochschild’s research, Sanders observes that sex workers create “manufactured identities” both to protect themselves from the psychological risks of the job and as a business strategy, and McLean, working through Minichiello and Browne, extends this claim to account for the additional sexual safety practices used by male sex workers.⁵⁷ The participants in my study detail a series of linguistic methods they use to establish and maintain these manufactured identities on SNS platforms. Drawing on their responses, I extend an analysis of the rhetorical strategies these individuals use to create separate personas within and between digital publics in order to avoid Marwick and boyd’s phenomenon of context collapse.

Eighteen participants stated that they use a pseudonym when engaging in sex work. Two provided caveats, stating “yes, most of the time,” and “shortened form of my real name.” Two others indicated that they use a variety of pseudonyms, explaining, “Yes—multiple names,” and “Yes. One primary, several variations in fact. I would never ever use my real name.” One responded that she did so both to protect her privacy and create a mental barrier (similar to that indicated by Sanders):

Yes, I do. This is for the sake of privacy. My real name is ethnic and therefore unique, and combined with knowledge of what state I’m from, people could find who I am and where I live with minimal effort. This is also for the sake of separating my work from my personal life. Names are largely personal, so having a separate one for sex work helps me mentally separate clients from friends.

Another’s response operated in accordance with Hochschild’s writing on sex work as “surface acting.”⁵⁸ He stated, “I use a pseudonym that sounds legitimate. And I DO adopt a persona . . . in a sense. It’s akin to an actor who’s playing the role of a prostitute.” A third, who identifies as a transgender male, cited using alternate gender performance as part of his manufactured persona: “Yes, as a sex worker, my persona is a Cisgender Female, with alternative name.” While there are many reasons to use a pseudonym, a unifying thread that runs through these responses is the desire to protect an authentic digital identity.

Bennett describes a panopticon effect on SNS users: “Data subjects’ might not be monitored at any one time, but they would be well advised to behave as if they were.”⁵⁹ In response to this form of surveillance, sex workers implement a strategy of identity management as they move between digital publics. I asked the participants about the words and language (e.g. name, job title, mention of sex work) that they use to describe themselves on personal networking sites and the sites they use to discuss sex work. Seven participants stated directly that they use all or part of their legal name on personal

networking sites, such as Facebook, and only two responded that they use a pseudonym on these sites. Conversely, twelve participants reported that they use a pseudonym or handle on sites that they use to discuss sex work, such as FetLife, and only one responded that he uses his real name. In this way, sex workers' manufactured identities translate directly into digital publics through their use of naming conventions. One participant clarified, "My social orientation is straight, so I function in my personal world in that context . . . I keep my work strictly out of the public spotlight. (I live in the bible belt. Gay sex and prostitution are 2 of the biggest cultural taboos) Among a close circle of trusted friends, I'm pretty open and comfortable with direct references to what I do." His response suggests that it is not only the corporations or law enforcement that monitor his behavior, but other members of the digital publics who live in his local community.

The participants' digital identities are further cemented through the language used to talk about their profession on different sites. When discussing their work on sites such as Facebook, many participants emphasized that they refer only to the legal forms, such as pro-domme work (i.e. being paid to assume the dominant role in BDSM play), or else use coded language, such as "escort," "sexual healer," "spiritual healing," "bodywork," "massage," etc. to define their labor. Two participants clearly articulated the distinction between publics. One indicated that she uses a legal name and a "vanilla" job title on Facebook, but a pseudonym on FetLife, the site on which she references sex work in her writing and groups. Another noted, "I use my legal name on Facebook and Pinterest and my common scene name on Fetlife. My personal Fetlife account references and links to my sex work account. My sex work name includes my scene name, so that perspective clients [sic] can vet me in the community," and further clarified that, on the sites they use to discuss sex work, "I use a pseudonym. I refer to myself directly as a Domme and fetish model and am careful to use language that's legal." Although a counterpublic like FetLife is a safer space for sex workers to discuss their labor than a normative public like Facebook, it still operates in accordance with US legislation, and members must be careful to use language that falls within the legal limits.

In describing the digital personae created by user data, Lyon claims, "the data doubles, created as they are from coded categories, are not innocent or innocuous virtual fictions. As they circulate, they serve to open and close doors of opportunity and access."⁶⁰ The participants in this study create multiple data doubles across different SNS platforms. In doing so, they gain access to the opportunities offered by normative publics like Facebook (e.g. connections to friends and family, networks to disseminate information, etc.) as well as those offered by counterpublics such as FetLife (e.g. communication with other sex workers and those in the kink community). In addition to using linguistic and rhetorical strategies to keep these identities separate, participants also indicate a variety of technological methods.

Surveillance, Privacy, and Cyber Security

Surveillance is inherent to web 2.0. Members of digital publics are constantly surrendering their data to corporations on a micro and macro level (what Clarke refers to as "dataveillance"), as well as to other members of the publics to which they belong (what Jansson et al. refer to as "interveillance").⁶¹ Fuchs explains that as companies continue to profit from user data, the lines between these forms of surveillance continue to blur, and Cohen demonstrates that regulations that protect user privacy in online publics are often written to accommodate big data collection.⁶² Thus, while many SNS platforms will provide users with privacy settings, which allow members to influence which and how much data is displayed within the public (providing protection on the level of interveillance), the site itself still controls access to the user's data (further supporting the tendency toward dataveillance). In addition to these overarching issues, sex workers face

the added threats of social stigma, online harassment, and law enforcement. For this vulnerable population, online privacy is a practical rather than theoretical concern. In discussing the options that websites do provide to opt out of targeted ads, Fuchs reminds us, "Not all users have excellent Internet usage skills, which is an aspect of digital inequality."⁶³ This observation is reflected in the survey responses as participants indicated a spectrum of privacy practices that require varying levels of technological knowledge and skill to execute.

Fourteen participants responded that they take additional measures to protect their privacy online. Several of them indicated straightforward "cyber hygiene" tactics that require conscious attention but little technological knowledge. Three participants noted that they "avoid crossing photos between identities." One participant specifically stated that she does not show her face in the pictures that she uses for sex work and does not use these photos elsewhere. This tactic only requires members of digital publics to remember which photos they have uploaded to each public. Another took photo security a step further, blending the digital with the material. She stated that she scrubs EXIF data off all photos before posting them on SNS platforms and uses "costumes, wigs, and makeup" in the photos she uses for sex work. This participant and one other referenced geographical location, claiming that they are careful to avoid providing any information that could reveal where and with whom they live when engaging in online sex work. Because sites like FetLife do not require members to input their location, this procedure is easily executable. One participant additionally remarked, "Deleting emails regularly, leaving the inbox and trash as clean as a whistle." Although some sites save messages exchanged between members as a form of dataveillance, this provision would help this individual avoid accidental detection on the level of interveillance. Such precautions show an awareness of many of the most common digital threats.

Participants also reported using technologies that require a basic level of knowledge or skill. One participant responded that they use "incognito mode" to communicate with clients and avoid linking their Facebook and Google accounts to their work email and persona. While this prevents information regarding a user's browsing history, cookies, and logins from being stored, it does not provide full protection from dataveillance as the user may still be visible to websites that they visit, institutions that provide them access, and internet service providers. Five participants marked that they use a different or virtual phone number, and four stated that they used a different or unlinked email. Tools such as these are free and readily available to the public. For instance, Google Voice allows users to acquire a free phone number from any available US city; however, its program policy does state, "Do not use Google Voice to engage in or promote illegal activities."⁶⁴ Though users gain an added layer of privacy, they do so by taking on an added element of risk in breaking the law, violating the site's Terms of Service, and making themselves more available to Google's databases. One participant takes these technologies a step further and uses a "burner phone," thereby acknowledging the importance of using secure hardware as well as secure software.

In addition to these fairly straightforward methods, other more powerful tools are used with a fair amount of frequency. Six participants indicated that they used a VPN, or Virtual Private Network. These tools enable users to send data across public networks, through other computers called "proxies," without connecting it to their IP addresses. An EFF whitepaper notes that police typically trace IP addresses as a way to solve crimes, often at a great risk to the subject's privacy.⁶⁵ However, privacy tools that prevent this require money and technical skill to implement. One user participant stated that her husband reroutes their browsing, and further clarified that she did not understand this process. Their response indicates that some digital privacy methods, especially those that protect

users against dataveillance, may be inaccessible to users without computational knowledge, and underscores the importance of having a support network in these instances. Participants indicated other cyber security tactics that intervene on the level of dataveillance; however, these were used with somewhat less frequency than or in accordance with a VPN. One participant who uses a VPN also noted using, “IP anonymizers, proxies, firewalls, airgap measures,” but did not explain these tactics further. Another VPN user stated, “I’m just beginning to experiment with crypto currency paymebts [sic].” Such measures would protect the user from unwanted intruders accessing their computer and from alerting companies, such as PayPal, and law enforcement to suspicious payments respectively. One participant, who does not use a VPN, reported that they use TOR, a secure browser, and TAILS, an anonymous OS that can be launched from a USB stick or DVD from almost any computer. Again, such practices protect the user from both intrusion and detection, but require a higher level of computational knowledge and skill.

Citing Stalder, Bennett claims, “Privacy is not the ‘antidote to surveillance’ nor was it ever meant to be.”⁶⁶ Indeed, for the computer user, perfect privacy is an ever-receding horizon. For vulnerable populations like online sex workers, however, surveillance is not an abstract concern, but a real threat to one’s livelihood, and privacy not a theoretical aim, but a practical necessity. For the participants in this study, privacy begins in public. These individuals consciously discern between digitally networked publics and counterpublics as places where they can and cannot discuss their labor. They then use naming conventions and rhetorical strategies to manufacture and maintain separate identities within each public. In order to further protect themselves from dataveillance and interveillance, they use a variety of cyber security tactics that require varying levels of technological knowledge and skill to implement. Privacy is not an act that happens once but a process that these individuals must repeatedly perform.

Conclusion

In this article, I have extended the scholarship on digitally networked publics to account for normative publics and counterpublics. I have claimed that Facebook operates as a normative public and FetLife as a counterpublic due to their approaches to data collection and implementation of US legislation regarding sex work within their site policies. Building on previous research regarding online sex work, I have offered a new study that considers the ways in which online sex workers use site selection, self presentation, cyber security, and cyber hygiene to establish and maintain manufactured identities within these publics as a means of combatting the surveillance inherent to web 2.0.

An obvious limitation to this study is the sample size. Generalizations about a population cannot be made from a sample of twenty-five participants. Using a larger sample, future research should consider the roles that the identity categories of class, race, gender, and sexual orientation play in online sex workers’ approach to privacy. Additional lines of inquiry might also address how surveillance capitalism benefits from this specific population, the ways in which anti-sex work legislation and policy adapt to sex workers’ privacy practices as well as the political implications of examining vulnerable populations within academic studies. By examining the privacy practices of those for whom surveillance is an immediate threat, we can develop a security model that is applicable more broadly to all members of digital publics.

Notes




1. Alice Marwick and danah boyd, “I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience,” *New Media & Society* 13, no. 1

2. Christopher W. Blackwell and Sophia F. Dziegielewska, "Risk for a Price: Sexual Activity Solicitations in Online Male Sex Worker Profiles," *Journal of Social Service Research* 39, no. 2 (2013): 159, doi:10.1080/01488376.2012.744617; Jesse Drucker and Tanya Nieri, "Female Online Sex Workers' Perceptions of Exit from Sex Work," *Deviant Behavior* (2016): 1, doi:10.1080/01639625.2016.1257890. [↗](#)
3. Niels Brügger, "A Brief History of Facebook as a Media Text: The Development of an Empty Structure," *First Monday* 20, no. 5 (2015), doi:10.5210/fm.v20i5.5423. [↗](#)
4. Facebook, Inc., Facebook, 2018, Accessed November 26, 2018, <https://www.facebook.com/>. [↗](#)
5. José Van Dijck, "'You Have One Identity': Performing the Self on Facebook and LinkedIn," *Media, Culture & Society* 35, no. 2 (2013): 200, doi:10.1177/0163443712468605. [↗](#)
6. Christian Fuchs, "New Media, Web 2.0 and Surveillance," *Sociology Compass* 5, no. 2 (2011): 138–41, doi:10.1111/j.1751-9020.2010.00354.x. [↗](#)
7. Damien Fay, Hamed Haddadi, Michael C. Seto, Han Wang, and Christoph Kling, "An Exploration of Fetish Social Networks and Communities," *Advances in Network Science*, Lecture Notes in Computer Science (New York: Springer, 2016), 198, doi:10.1007/978-3-319-28361-6_17. [↗](#)
8. BitLove, Inc., FetLife, 2018, Accessed November 26, 2018, <https://fetlife.com/>. [↗](#)
9. Michael Warner, *Publics and Counterpublics* (New York: Zone Books, 2002), 67. [↗](#)
10. danah boyd, "Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications," in *A Networked Self: Identity, Community, and Culture on Social Network Sites*, ed. Zizi Papacharissi (New York: Routledge, 2010), 42. [↗](#)
11. Marwick and boyd, 122–123. [↗](#)
12. Van Dijck, "You Have One" 200. [↗](#)
13. Warner, *Publics*, 63. [↗](#)
14. Warner, *Publics*, 112–113. [↗](#)
15. André Jansson, Mia Lövheim, Susanna Paasonen, and Johanna Sumiala, "Social Media: Implications for Everyday Life, Politics and Human Agency," *Approaching Religion* 3, no. 2 (2013): 29, doi:10.30664/ar.67514. [↗](#)
16. Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75–89, doi:10.1057/jit.2015.5. [↗](#)
17. Fuchs, "New Media," 138. [↗](#)
18. BitLove, Inc., FetLife. [↗](#)
19. BitLove, Inc., FetLife. [↗](#)
20. Alexandra Lutnick and Deborah Cohan, "Criminalization, Legalization Or Decriminalization of Sex Work: What Female Sex Workers Say in San Francisco, USA," *Reproductive Health Matters* 17, no. 34 (2009): 38; *West's Encyclopedia of American Law*, 2nd ed., s.v. "Prostitution." [↗](#)
21. Jacqueline Comte, "Decriminalization of Sex Work: Feminist Discourses in Light of Research," *Sexuality & Culture* 18, no. 1 (2013): 202, doi:10.1007/s12119-013-9174-5; Kamala Kempadoo, Jyoti Sanghera, and Bandana Pattanaik, *Trafficking and Prostitution Reconsidered: New Perspectives on Migration, Sex Work, and Human Rights* (London: Routledge, 2012): 151. [↗](#)
22. The United States Department of Justice, "Model State Provisions on Pimping, Pandering, and Prostitution," The United States Department of Justice, 2014,

accessed November 26, 2018, <https://www.justice.gov/olp/model-state-provisions-pimping-pandering-and-prostitution>. ↗

23. Alexandra Murphy and Sudhir Alladi Venkatesh, "Vice Careers: The Changing Contours of Sex Work in New York City," *Qualitative Sociology* 29 (2006): 137. ↗
24. Elliot Harmon, "How Congress Censored the Internet," Electronic Frontier Foundation, March 24, 2018, <https://www.eff.org/deeplinks/2018/03/how-congress-censored-internet>. ↗
25. Emily Witt, "After the Closure of Backpage, Increasingly Vulnerable Sex Workers Are Demanding Their Rights," *The New Yorker*, June 10, 2018, Accessed November 26, 2018, <http://www.newyorker.com/news/dispatch/after-the-closure-of-backpage-increasingly-vulnerable-sex-workers-are-demanding-their-rights>. ↗
26. Facebook, Inc., Facebook. ↗
27. BitLove, Inc., FetLife. ↗
28. Alison Bass, *Getting Screwed: Sex Workers and the Law* (Lebanon, NH: ForeEdge, An imprint of University Press of New England, 2015): 45; Elizabeth Bernstein, *Temporarily Yours: Intimacy, Authenticity, and the Commerce of Sex* (Chicago: University of Chicago Press, 2008): 69; Angela Jones, "Sex Work in a Digital Era," *Sociology Compass* 9, no. 7 (2015): 560, doi:10.1111/soc4.12282. ↗
29. Drucker and Nieri, "Female Online," 1. ↗
30. Cecilie Høigård and Liv Finstad, *Backstreets: Prostitution, Money, and Love* (Cambridge: Polity Press, 1992): 183–184; Carole S. Vance, *Pleasure and Danger: Exploring Female Sexuality* (London: Pandora, 1992). ↗
31. Jacqueline Comte, "Decriminalization of Sex Work: Feminist Discourses in Light of Research," *Sexuality & Culture* 18, no. 1 (2013): 197–199, doi: 10.1007/s12119-013-9174-5; Ronald Weitzer, "New Directions in Research on Prostitution," *Crime, Law and Social Change* 43, no. 4–5 (2005): 213, doi:10.1007/s10611-005-1735-6. ↗
32. Kevin Walby, *Touching Encounters: Sex, Work, and Male-for-male Internet Escorting* (Chicago, Ill: University of Chicago Press, 2012). ↗
33. Drucker and Nieri, "Female Online," 1. ↗
34. Jones, "Sex Work in a Digital Era," 560. ↗
35. Bass, *Getting Screwed*, 45; Drucker and Nieri, "Female Online," 1. ↗
36. Jones, "Sex Work in a Digital Era," 560. ↗
37. Jones, "Sex Work in a Digital Era," 560; Tammy Castle and Jenifer Lee, "Ordering Sex in Cyberspace: A Content Analysis of Escort Websites," *International Journal of Cultural Studies* 11, no. 1 (2008), doi:10.1177/1367877907086395; Scott Cunningham and Todd D. Kendall, "Prostitution 2.0: The Changing Face of Sex Work," *Journal of Urban Economics* 69, no. 3 (2011); Thomas J. Holt and Kristie R. Blevins, "Examining Sex Work from the Clients Perspective: Assessing Johns Using On-line Data," *Deviant Behavior* 28, no. 4 (2007), doi:10.1080/01639620701233282; Matthew V. Pruitt, "Online Boys: Male-for-Male Internet Escorts." *Sociological Focus* 38, no. 3 (2005), doi:10.1080/00380237.2005.10571265; Quinn, James F., and Craig J. Forsyth. "Describing Sexual Behavior in the Era of the Internet: A Typology for Empirical Research." *Deviant Behavior* 26, no. 3 (2005), doi:10.1080/01639620590888285; Weitzer, "New Directions." ↗
38. Holt and Blevins, "Examining Sex Work," 343–344. ↗
39. Blackwell and Dziegielewski, "Risk for a Price"; Andrew McLean, "New Realm, New Problems? Issues and Support Networks in Online Male Sex Work," *Gay & Lesbian Issues and Psychology Review* 8, no. 2 (2012): 70-81; Pruitt, "Online Boys." ↗
40. Jones, "Sex Work in a Digital Era," 565. ↗

41. Bass, *Getting Screwed*, 55; Castle and Lee, "Ordering Sex," 108; Drucker and Nieri, "Female Online," 2; Jones, "Sex Work in a Digital Era," 561; Weitzer, "New Directions," 216. [↗](#)
42. Blackwell and Dziegielewski, "Risk for a Price," 160; Cunningham and Kendal, "Prostitution 2.0," 276. [↗](#)
43. McLean, "New Realm," 76. [↗](#)
44. Angela Jones, "I Get Paid to Have Orgasms': Adult Webcam Models' Negotiation of Pleasure and Danger," *Signs: Journal of Women in Culture and Society* 42, no. 1 (2016): 240–243, doi:10.1086/686758. [↗](#)
45. Bass, *Getting Screwed*, 53, 58–59. [↗](#)
46. Bass, *Getting Screwed*, 44, 56. [↗](#)
47. McLean, "New Realm," 71; Teela Sanders, "Its Just Acting: Sex Workers Strategies for Capitalizing on Sexuality," *Gender, Work and Organization* 12, no. 4 (2005): 319–42, doi:10.1111/j.1468-0432.2005.00276.x. [↗](#)
48. Jones, "Sex Work in a Digital Era," 564. [↗](#)
49. Matt Brim and Amin Ghaziani, "Introduction: Queer Methods." *WSQ: Women's Studies Quarterly* 44, no. 3–4 (2016): 16, doi:10.1353/wsq.2016.0033. [↗](#)
50. Caroline Dadas, "Messy Methods: Queer Methodological Approaches to Researching Social Media," *Computers and Composition* 40 (2016): 60–72, doi:10.1016/j.compcom.2016.03.007. [↗](#)
51. Angela Jones, "Pornographics as Queer Method," in *Other, Please Specify: Queer Methods in Sociology*, ed. DLane R. Compton, Tey Meadow, and Kristen Schilt (Oakland, CA: University of California Press, 2018), 104. [↗](#)
52. Suzanne Jenkins, "New Technologies, New Territories: Using the Internet to Connect with Sex Workers and Sex Industry Organizers," in *New Sociologies of Sex Work*, ed. Kate Hardy, Sarah Kingston, and Teela Sanders (Farnham: Ashgate, 2011), 92. [↗](#)
53. McLean, "New Realm," 72. [↗](#)
54. Jansson et al., "Social Media," 30. [↗](#)
55. Christian Fuchs, "Social Software and Web 2.0: Their Sociological Foundations and Implications," in *Handbook of Research on Web 2.0, 3.0, and X.0: Technologies, Business, and Social Applications*, ed. San Murugesan and San Murugesan (Hershey, PA: Information Science Reference, 2010), 764–89. [↗](#)
56. Colin J. Bennett, "In Defense of Privacy: The Concept and the Regime," *Surveillance & Society* 8, no. 4 (2011): 490, doi:10.24908/ss.v8i4.4184. [↗](#)
57. McLean, "New Realms," 72; Sanders, "Its Just Acting," 323. [↗](#)
58. Arlie Russell Hochschild, *The Managed Heart: Commercialization of Human Feeling* (Berkeley: University of California Press, 1983). [↗](#)
59. Bennett, "In Defense," 492. [↗](#)
60. David Lyon, *Surveillance and Social Sorting: Privacy, Risk and Digital Discrimination* (Routledge, 2003), 27. [↗](#)
61. Roger Clarke, "Dataveillance: Delivering '1984,'" in *Framing Technology: Society, Choice, and Change*, ed. Lelia Green and Roger Guinery, 117–30 (St. Leonards, N.S.W.: Allen & Unwin, 1994); Jansson et al., "Social Media," 34. [↗](#)
62. Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012), 10; Fuchs, "New Media, Web 2.0 and Surveillance," 138. [↗](#)
63. Fuchs, "New Media, Web 2.0 and Surveillance," 142. [↗](#)

64. Google LLC, "Google Voice Acceptable Use Policy," Google Voice, accessed November 26, 2018, <https://www.google.com/intl/en-US/googlevoice/program-policies.html>. 
65. Aaron Mackey, "Unreliable Informants: IP Addresses, Digital Tips and Police Raids," Electronic Frontier Foundation, May 16, 2017, 7–8, <http://www.eff.org/wp/unreliable-informants-ip-addresses-digital-tips-and-police-raids>. 
66. Bennett, "In Defense," 493. 

 [Bio](#)

S. L. Nelson

S.L. Nelson studies rhetoric and composition at the University of Pittsburgh. Their research examines the slippage and play that occurs within the rhetoric of computational structures. Working through queer theoretical and methodological frameworks, they consider the ways in which computer users can critique, resist, and subvert the normative narratives perpetuated by digital systems.



This work is licensed under a Creative Commons Attribution 4.0 International (CC BY) License, unless otherwise noted.
ISSN 2469-4053